REMARKS

Claims 8 – 13, 16, 18, 19, 21, 22, 24, 25, 27, 32, and 33 are pending. Claims 1 – 5 and 28 - 30 have been cancelled. Claims 32 and 33 have been added. Claims 8, 16, 22, 24, 25, and 27 have been amended. No new matter has been added. Reexamination and reconsideration of the present application are respectfully requested.

In the July 12, 2005 Office Action, the Examiner rejected claims 1 – 5, 8 – 13, 16, 18, 19, 21, 22, 24, 25, and 27 - 30 under 35 U.S.C. § 103(a) as being unpatentable over Krishna (WO 01/05086) in view of Johnson et al. (US Patent No. 6,754,755). This rejection is respectfully traversed in so far as they are applicable to the presently pending claims.

Claim 16 recites:

> A method of decrypting an encrypted packet received by a computing system, comprising:
> receiving said encrypted packet from a network and transferring said encrypted packet to a host memory;
> **issuing a decryption command to a controller;**
> **specifying an average latency value to the controller;**
> **waiting the average latency value before said assertion of an interrupt in response to said decryption command;**
> transferring said encrypted packet to said controller;
> converting said encrypted packet to a decrypted packet; and
> transferring said decrypted packet to the host memory, **wherein the interrupt is asserted at a time before completing said transfer of said decrypted packet to said host memory**.

The Krishna reference does not disclose, teach, or suggest the method of claim 16. The Examiner states that the Krishna reference discloses the "issuing a decryption command to a controller" limitation because the Krishna reference discloses that the system includes a processor which controls the sequencing and processing of packets. The applicants respectfully disagree with the Examiner. The Examiner is not identifying

whether the processor in the distributor unit is the controller of claim 16. If the processor in the distributor unit is the controller recited in claim 16, then the Krishna processor is issuing commands and not receiving the decryption command, as is recited in claim 16. If the Examiner is identifying that the processor in the distributor unit is issuing commands, the Examiner has not identified that a command has been issued to a controller, as is recited in claim 16.

The Examiner states that the Krishna reference does not mention (or disclose) **a time for assertion of an interrupt in response to said decryption command or asserting an interrupt at a time before completing said transfer of said decrypted packet to said host memory**, as are all recited in claim 16. The applicants agree with the Examiner. In addition, the applicants note that the Krishna reference does not disclose **specifying an average latency value to the controller.** Accordingly, applicants respectfully submit that claim 16 distinguishes over the Krishna reference because the Krishna reference does not expressly disclose any of the above-highlighted limitations of claim 16.

The Johnson reference does not make up for the deficiencies of the Krishna reference. The Examiner states that the Johnson reference in Figs. 5 and 6 and columns 8 – 10 discloses the highlighted limitations. *(Office Action, pages 7 – 8)*. The applicants respectfully disagree with the Examiner. The applicants first note that the Johnson reference is not disclosing, in columns 9 and 10, decryption of packets and processing **decrypted** packets at a controller. Instead, the Johnson reference is disclosing the processing of packets and then transferring the packets to memory. This corresponds to the first limitation of claim 16. There is no disclosure of encryption and

decryption of packets.

In an embodiment of the invention, the Johnson reference discloses that a possible solution is to determine an approximate interrupt latency period of the computer system on the network and cause the interrupt logic of the NIC to assert an interrupt early in the approximate latency period. For example, during the receive operation, the NIC receives the packet from the network and transfers the packet to system memory 206. Normally, the NIC waits until a packet is completely transferred to the system memory before asserting an interrupt. For an early interrupt, the NIC calculates the approximate time, called the packet transfer time, for the packet to be completely transferred to the system memory using the packet size and a measured or determined transfer rate. The NIC subtracts the latency period from the packet transfer time to determine a delay time after the start of packet transfer. The NIC then asserts the interrupt early after the expiration of the delay time. *(Johnson, col. 9, lines 22 – 40).*

This is not the same as a method of decrypting an encrypted packet received by a computing system, including receiving said encrypted packet from a network and transferring said encrypted packet to a host memory, **issuing a decryption command to a controller, specifying an average latency value to the controller, and waiting for the average latency value before said assertion of an interrupt in response to said decryption command.** The Johnson reference does not disclose issuing a decryption command because the Johnson reference is not directed to transferring of encrypted packets. In addition, the Johnson reference discloses that the NIC calculates a packet transfer time and subtracts the latency period (i.e., the time when the interrupt is asserted until when the processing logic handles the interrupt) from the packet

transfer time to create a delay time. This is not the same as a specifying an average latency to a controller because the Johnson reference is not disclosing that an average latency is calculated, as is recited by claim 16. Instead, the Johnson reference is disclosing that a specific time is calculated each time by the NIC.

Further, the Johnson reference is not disclosing a method including **waiting for the average latency value before said assertion of an interrupt in response to said decryption command.** The Johnson reference does not disclose that the interrupt is in response to a decryption command, as is recited in claim 16. Instead, the Johnson reference interrupt is generated in response to the transferring of packets into the main memory and not in response to a decryption command. In addition, as noted above, there is no disclosure that the Johnson reference calculates an average latency value, and therefore the Johnson reference does not disclose waiting for the average latency value before assertion of the interrupt, as is recited in claim 16.

Finally, the Johnson reference does not disclose transferring said decrypted packet to the host memory, **wherein the interrupt is asserted at a time before completing said transfer of said decrypted packet to said host memory.** The Johnson reference is not disclosing the transferring of a decrypted packet because the Johnson reference does not disclose working with encrypted or decrypted packets or all. The Johnson reference is only disclosing what happens when the packet is first received, which is similar to the first limitation of claim 16, and does not deal with the transferring of said decrypted packet back to the host memory. Accordingly, claim 16, as amended, further distinguishes over the Johnson reference, alone or in combination with the Krishna reference.

Independent claims 8 and 22, both as amended, recite limitations similar to claim 16. Accordingly, applicants respectfully submit that claims 8 and 22 distinguish over the Krishna / Johnson combination for reasons similar to those discussed above in regard to claim 16.

Claims 9 – 13, 18, 19, 21, 24, 25, 27, 32, and 33 depend, directly or indirectly, on claims 8, 16, and 22. Accordingly, applicants respectfully submit that claims 9 – 13, 18, 19, 21, 24, 25, 27, 32, and 33 distinguish over the Krishna / Johnson combination for the same reasons as those discussed above in regard to claim 16, as amended.

Claim 32 further distinguishes over the cited references. Claim 32 recites:

> The method of claim 16, further including asserting the interrupt before the encrypted packet is fully decrypted.

Neither of the Krishna reference nor the Johnson reference discloses that the interrupt is asserted before the encrypted packet is fully decrypted. The Krishna reference does not disclose the asserting of an interrupt during the processing of the encrypted packet. The Johnson reference discloses interrupts, but there is no disclosure that the interrupt is asserted before the encrypted packet is fully decrypted because the Johnson reference does disclose encryption or decryption. Accordingly, claim 32 further distinguishes over the Krishna / Johnson combination.

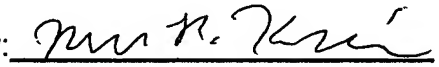
Claim 33 recites limitations similar to claim 32. Accordingly, applicants respectfully submit that claim 33 further distinguishes over the Krishna / Johnson combination for reasons similar to those discussed above in regard to claim 32.

Applicants believe that the foregoing remarks place the application in condition for allowance, and a favorable action is respectfully requested. If for any reason the Examiner finds the application other than in condition for allowance, the Examiner is requested to call the undersigned attorney at the Los Angeles telephone number (213) 488-7100 to discuss the steps necessary for placing the application in condition for allowance should the Examiner believe that such a telephone conference would advance prosecution of the application.

Respectfully submitted,

PILLSBURY WINTHROP SHAW PITTMAN LLP

Date: May 22, 2006

By: 

Mark R. Kendrick
Registration No. 48,468
Attorney for Applicant(s)

725 South Figueroa Street, Suite 2800
Los Angeles, CA 90017-5406
Telephone: (213) 488-7100
Facsimile: (213) 629-1033